SOME APPLICATIONS OF QUANTUM INFORMATION THEORY IN INTERACTIVE QUANTUM COMMUNICATION

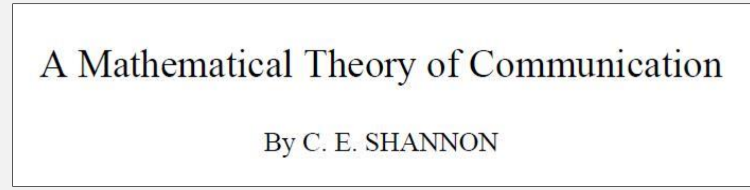
PENGHUI YAO

NANJING UNIVERSITY

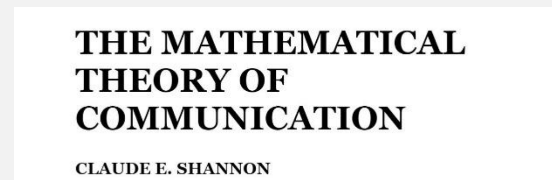
ITU WORKSHOP ON QUANTUM INFORMATION TECHNOLOGY (QIT) FOR NETWORKS

Entropy

$$H(X) \coloneqq \sum_{x} \Pr[X = x] \log \frac{1}{\Pr[X = x]}$$


A Mathematical Theory of Communication

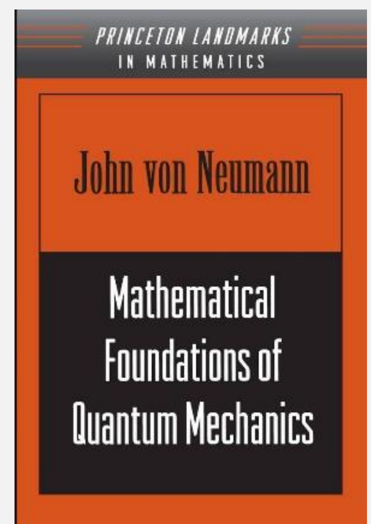
By C. E. SHANNON


THE MATHEMATICAL THEORY OF COMMUNICATION

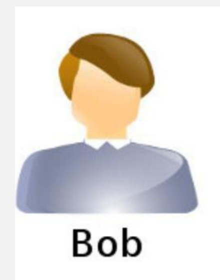
CLAUDE E. SHANNON

Von Neumann Entropy

$$S(\rho) \coloneqq -Tr\, \rho \log \rho$$



SHANNON'S NOISELESS CODING THEOREM



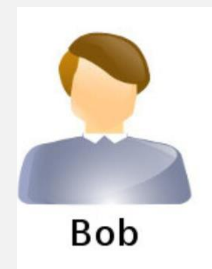
$x_1, x_2, \ldots, x_n \sim X$

n · H(X) bits

Shannon's source coding theorem:

$$\lim_{n\to\infty} C_n(X)/n = H(X)$$

EXAMPLE OF ONE-SHOT INFORMATION THEORY



$x \sim X$

[Huf 1952]Huffman coding: expected length $\leq H(X) + 1$

QUANTUM NOISELESS CODING THEOREM

$\mathrm{n} \cdot \mathrm{S}(\rho)$ bits

$$\rho \otimes \rho \otimes \cdots \otimes \rho$$

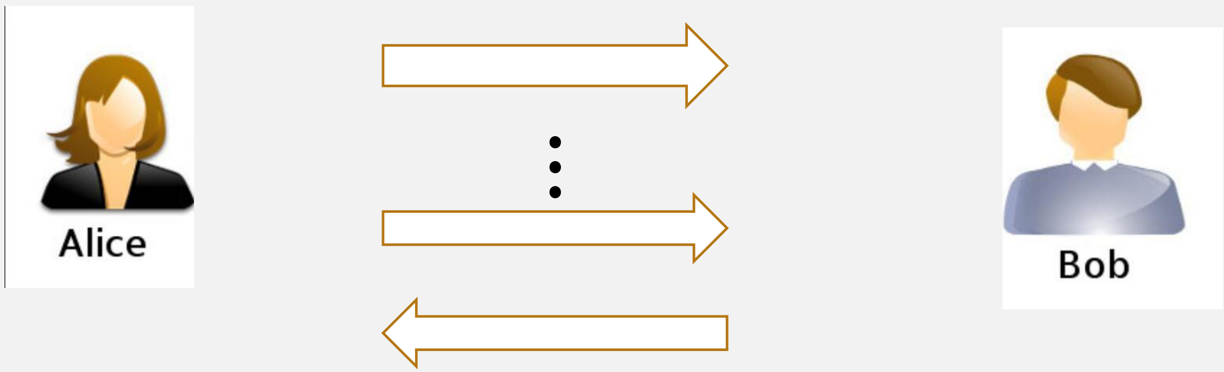
Holevo-Schumacher-Westmoreland Theorem

$$\lim_{n \to \infty} C_n(\rho)/n = S(\rho)$$

TRADITIONAL INFORMATION THEORY

- “studies the quantification, storage, and communication of information”
- Applications: compression, error-correcting codes, cryptography
- Major focus: one-shot / asymptotic and one-way data transmission

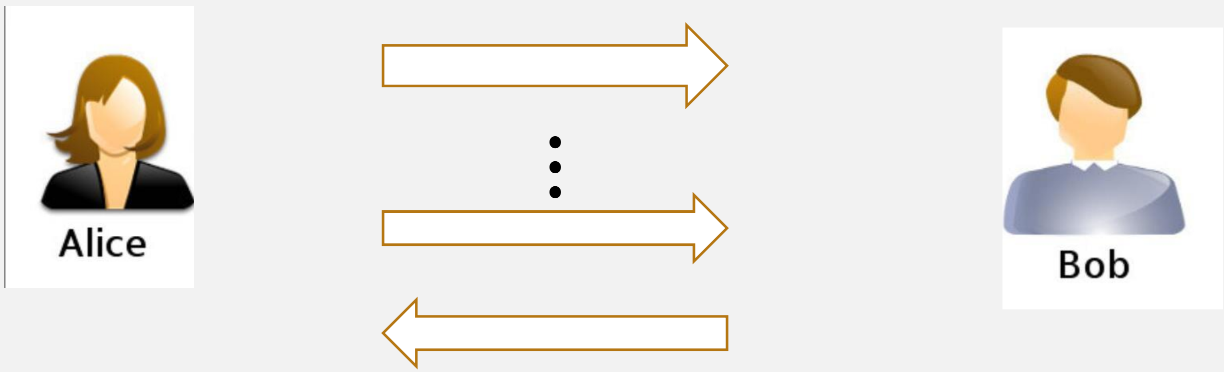
COMMUNICATION COMPLEXITY [YAO'79]



$x \sim X$ $y \sim Y$

$CC(f)$: the minimum # of bits to exchange to compute $f(x, y)$

INTERACTIVE CLASSICAL COMMUNICATION



$x \sim X$ $\qquad$ $y \sim Y$

- [Bra'10] Information complexity

$$\text{IC} := \frac{1}{2}\left(I(X : \text{mess}|Y) + I(Y : mess|X)\right)$$

- [BR'11] $\lim_{n\to\infty} CC(f^n)/n = IC(f)$

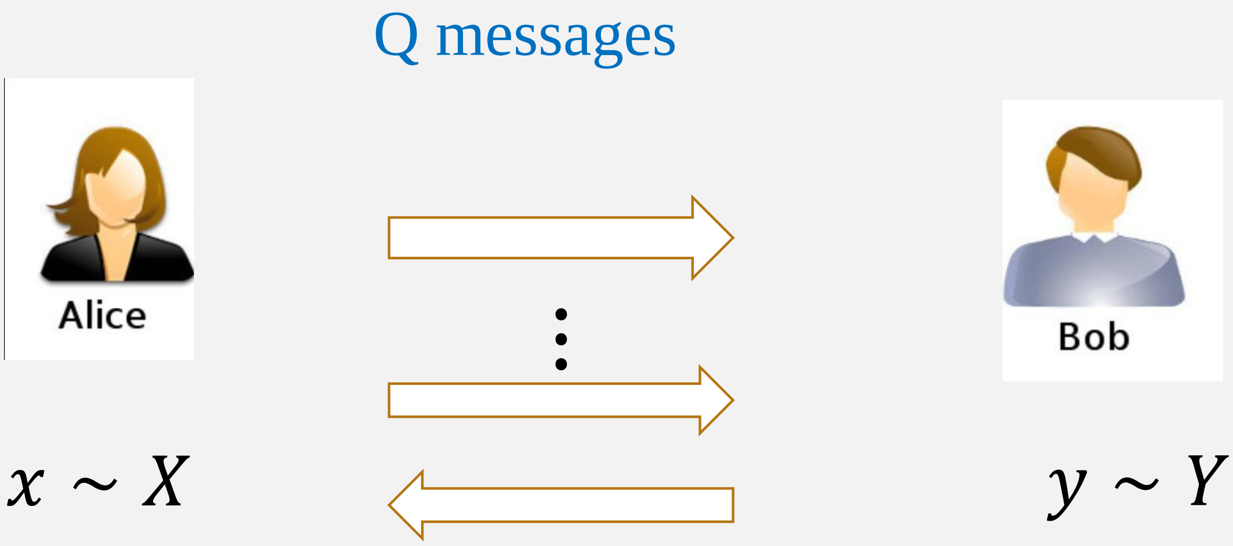
WHY INFORMATION COMPLEXITY

Message compression:

A C-bit interactive protocol with information complexity I, how much can we compress?

- Braverman et.al. $O(\sqrt{IC})$
- Braverman et.al. $O(I + O(\sqrt{r \cdot I} + r))$
- Braverman & Garg $O\left(2^{O(I)}\right)$
- For product inputs: Sherstov. $\tilde{O}(I)$

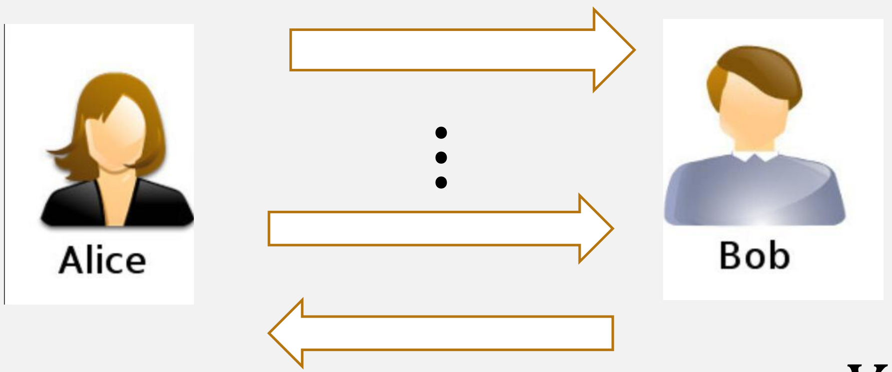
QUANTUM INFORMATION COMPLEXITY?



Q: Is it possible to compress a quantum interactive protocol?
How to define a quantum information complexity?

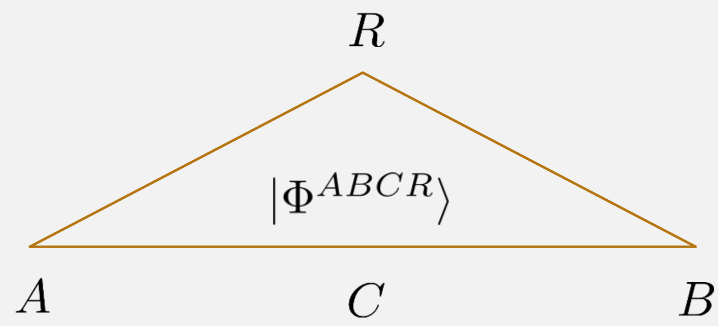
Messages do not exist at the same time due to non-cloning

QUANTUM INFORMATION COMPLEXITY?



$x \sim X$

$y \sim Y$



[YD'09] $QIC = \frac{1}{2} I(C:R|B)$

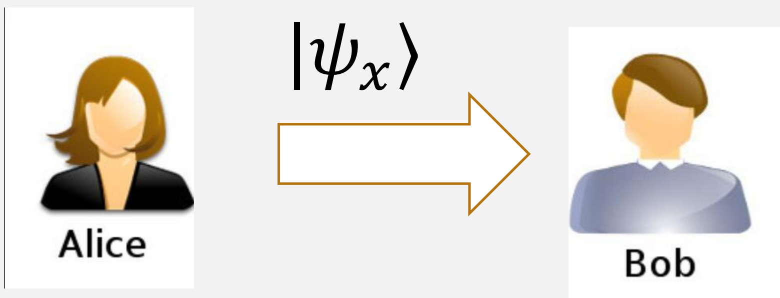
One step

[Tou'15] $QIC = \sum QIC$ (each step)

[Tou'15] $QIC(f) = \lim_{n\to\infty} QCC(f^n)/n$

COMPRESSION ALGORITHMS

$|\psi_x\rangle$

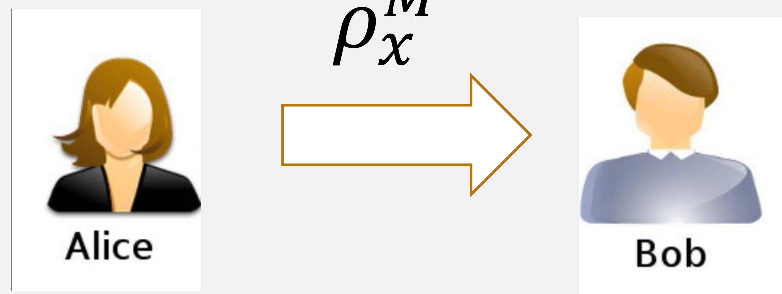


$x \sim X$

QIC=$S(E[|\psi_x\rangle\langle\psi_x|])$

[AGHY'18] There is no quantum Huffman coding!

ρ_x^M



$x \sim X$ $y \sim Y$

QIC=$I(X:M|Y)$

[AJMSY'18] $O\big(I(X:M|Y)\big)$ qubits are sufficient.

COMPRESS INTERACTIVE PROTOCOLS

A C-qubit quantum interactive protocol with quantum information complexity I, how much can we compress?

Can we compress it to I?

[ATYY'18] No! There exists a protocol which cannot be compressed below $2^{O(I)}$

Bad news? Yes/No.

COMPRESS INTERACTIVE PROTOCOLS

$$\exists\ f \text{ s.t. } QCC(f) \gg QIC(f) = \lim_{n\to\infty} QCC(f^n)/n$$

$$\Rightarrow QCC(f^{\mathrm{n}}) \ll n \cdot QCC(\mathrm{f})$$

Jointly computing n instances can be much more efficient than computing each one independently.

LEARN/UNLEARN COMPLEXITY

- [Tou'13] $QIC = CIC + CRIC$

CIC: amount of info the players learned

$CRIC$: the amount of info the players unlearned

For any classical protocol, CRIC is always 0.

SET DISJOINTNESS

Set-disjointness $(x, y) = 1$ iff $\exists i \; x_i = y_i = 1$

001010011011

010010100000

SET DISJOINTNESS

Set-disjointness $(x, y) = 1$ iff $\exists i\ x_i = y_i = 1$

$f = 1$

001010011011 010010100000

- [Raz’95] $CC(f) = \Omega(n)$

DISTRIBUTED GROVER

Set-disjointness $(x, y) = 1$ iff $\exists i\ x_i = y_i = 1$

Initial state: $\sum_i |i, 0, z\rangle$

$\sum_i |i, x_i, z\rangle$

$\sum_i |i, x_i, (y_i\ AND\ x_i)\rangle$

Final state: $\sum_i |i, 0, (y_i\ AND\ x_i)\rangle$

One step of Grover $\Rightarrow O(\sqrt{n}\log n)$ comm. suffices.

DISTRIBUTED GROVER

Set-disjointness f: $(x, y) = 1$ iff $\exists i\ x_i = y_i = 1$

- [AA'03] $QCC(f) = \Theta(\sqrt{n})$

AA-protocol, CIC = $\Theta(\sqrt{n})$ and CRIC = $\Theta(\sqrt{n})$

- [LT'17] For any q. protocol with CRIC=0, then QCC(f) = $\Theta(n)$

Unlearning info. is essential for quantum speedup.

FURTHER WORK

- Any nontrivial compression algorithms for quantum interactive protocols?
- Information complexity for multi-party quantum communication?
- The role of unlearning info. for other problems

Thank you